GENERALIZATIONS OF IWASAWA'S 'RIEMANN-HURWITZ' FORMULA FOR CYCLIC p-EXTENSIONS OF NUMBER FIELDS

JORDAN SCHETTLER

Abstract. We produce generalizations of Iwasawa's 'Riemann-Hurwitz' formula for number fields. These generalizations apply to cyclic extensions of number fields of degree p^n for any positive integer n. We use these formulas to establish a vanishing criterion for Iwasawa λ-invariants which generalizes a result of Takashi Fukuda et. al. We also take note of some congruences and inequalities.

1. Introduction

Fix a rational prime p and algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\mathbb{Q}_\infty \subseteq \overline{\mathbb{Q}}$ denote the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. In particular, we have

$$\mathbb{Q}_\infty \subseteq \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{p^n})$$

where ζ_{p^n} denotes a primitive p^nth root of unity. Following Iwasawa in [Iwa81], we define a $\mathbb{Z}_p$-field to be a finite extension of $\mathbb{Q}_\infty$. Equivalently, L is a $\mathbb{Z}_p$-field when $L = \ell\mathbb{Q}_\infty$ for some number field ℓ, so here L is the cyclotomic $\mathbb{Z}_p$-extension of ℓ. We define the ideal class group of a $\mathbb{Z}_p$-field L to be the quotient $C_L := I_L/P_L$ where I_L is the group of invertible fractional ideals of the integers $\mathcal{O}_L$ and P_L is the subgroup of principal fractional ideals.

Theorem 1 (Iwasawa, [Iwa59] and [Iwa73])**.** *Let L be a $\mathbb{Z}_p$-field and let A_L denote the p-primary part of the class group of L. Then there is an isomorphism of $\mathbb{Z}_p$-modules*

$$A_L \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L} \oplus M$$

where M has bounded exponent, i.e., $p^n M = 0$ for some n. In fact, if we write $L = \ell\mathbb{Q}_\infty$ for some number field ℓ, then the Iwasawa invariants $\lambda(L/\ell)$, $\mu(L/\ell)$ for the $\mathbb{Z}_p$-extension L/ℓ satisfy

(1) $\lambda(L/\ell) = \lambda_L$
(2) $\mu(L/\ell) = 0 \Leftrightarrow M = 0$.

In particular, this means that the vanishing of $\mu(L/\ell)$, as conjectured by Iwasawa, only depends on L, so we may write $\mu_L = 0$ to denote this.

In [Iwa81], Iwasawa used the above structure theorem and Galois actions on class groups to prove the following 'Riemann-Hurwitz' formula.

Theorem 2 (Iwasawa's 'Riemann-Hurwitz' Formula)**.** *Suppose L/K is a cyclic extension of $\mathbb{Z}_p$-fields of degree $[L : K] = p$. If L/K is unramified at the infinite*

places and $\mu_K = 0$, then $\mu_L = 0$ and

$$\lambda_L = [L : K]\lambda_K + (p-1)(h_2 - h_1) + \sum_{w \nmid p}(e(w) - 1) \tag{2.1}$$

where $e(w)$ denotes the ramification index in L/K of a place w of L not lying above p and for $i = 1, 2$ we write h_i for the $\mathbb{F}_p$-dimension of the cohomology group $H^i(\mathrm{Gal}(L/K), \mathcal{O}_L^\times)$.

2. The Euler Characteristic

We wish now to restate Iwasawa's formula 2.1 in a way which will lend itself more conveniently to generalization. We first state a definition.

Definition 3. Let G be a cyclic group of prime power order p^n. Suppose M is a G-module. We define the Euler characteristic $\chi(G, M) \in \mathbb{Z}$ to be the exponent of p in the Herbrand quotient

$$p^{\chi(G,M)} = \frac{|H^2(G, M)|}{|H^1(G, M)|}$$

when these quantities are finite.

Note that χ inherits the following properties (see [AT09]) directly from the Herbrand quotient:

(1) χ is additive on short exact sequences of G-modules
(2) $\chi(G, M) = 0$ when M is a finite G-module
(3) $\chi(G, M^*) = -\chi(G, M)$ when $M^* = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ is the p-Pontryagin dual of a $\mathbb{Z}_pG$-module M.

These properties and the techniques of [Iwa81] can be used to derive the following computations.

Lemma 4. *Suppose L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$. Then*

$$\chi(G, A_L) = -\chi(G, P_L) + \sum_{u \nmid p} \mathrm{ord}_p(e(w/u))$$

where $\mathrm{ord}_p(e(w/u))$ is the p-adic order of the ramification index in L/K for a finite place w of L lying over a place u of K which does not lie over p. If, in addition, L/K is unramified at every infinite place, then

$$-\chi(G, P_L) = \chi(G, \mathcal{O}_L^\times).$$

Corollary 5. *We can restate Iwasawa's formula 2.1 as*

$$\lambda_L = p\lambda_K + (p-1)\chi(G, A_L) \tag{5.1}$$

In fact, we need not assume that L/K is unramified at the infinite places for Equation 5.1 above to hold.

3. General Formulas

We will derive several generalizations of Iwsawa's formula, but first we need a couple of lemmas.

Lemma 6. *Let $G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ for some prime p and some positive integer n. Suppose M is a $\mathbb{Z}_pG$-module which is free of finite rank over $\mathbb{Z}_p$. Then there is a short exact sequence of $\mathbb{Z}_pG$-modules*

$$0 \to M' \to M \to \mathbb{Z}_p[\zeta_{p^n}]^{\oplus r} \to 0$$

where M' is a $\mathbb{Z}_p$-pure[1] $\mathbb{Z}_pG$-submodule of M which is annihilated by $g^{p^{n-1}} - 1$ and $\mathbb{Z}_p[\zeta_{p^n}]$ has $\mathbb{Z}_pG$-module structure given by

$$\mathbb{Z}_p[\zeta_{p^n}] \cong \frac{\mathbb{Z}_pG}{\Phi_{p^n}(g)\mathbb{Z}_pG}$$

with $\Phi_{p^n}(x) = p^n$th cyclotomic polynomial.

Proof. Define

$$M' := \{m \in M : (g^{p^{n-1}} - 1)m = 0\}.$$

Then M' is a $\mathbb{Z}_pG$-submodule of M since it is the kernel of a $\mathbb{Z}_pG$-homomorphism, namely, the multiplication by $g^{p^{n-1}} - 1$ map on M. We know M' is $\mathbb{Z}_p$-pure since if $rm = m'$ where $r \in \mathbb{Z}_p$, $m \in M$, and $m' \in M'$, then

$$r((g^{p^{n-1}} - 1)m) = (g^{p^{n-1}} - 1)(rm) = (g^{p^{n-1}} - 1)m' = 0,$$

so $(g^{p^{n-1}} - 1)m = 0$ (i.e., $m \in M'$) because M is $\mathbb{Z}_p$-torsion free. Also, M/M' is annihilated by $\Phi_{p^n}(g)$ since

$$(g^{p^{n-1}} - 1)(\Phi_{p^n}(g)m) = ((g^{p^{n-1}} - 1)(\Phi_{p^n}(g))m = (g^{p^n} - 1)m = 0$$

for all $m \in M$. Thus M/M' is a $\mathbb{Z}_p[\zeta_{p^n}]$-module which (since $M' \leq M$ is $\mathbb{Z}_p$-pure and $\mathbb{Z}_p$ is a PID) is free of finite rank over $\mathbb{Z}_p$. Note that $\mathbb{Z}_p \cap \mathbb{Z}_p[\zeta_{p^n}]\alpha$ is a non-zero ideal of $\mathbb{Z}_p$ when $0 \neq \alpha \in \mathbb{Z}_p[\zeta_{p^n}]$. Thus if $\alpha\overline{m} = 0$ for some $\overline{m} \in M/M'$, then $r\overline{m} = \beta(\alpha\overline{m}) = 0$ where $0 \neq r = \beta\alpha \in \mathbb{Z}_p$ for some $\beta \in \mathbb{Z}_p[\zeta_{p^n}]$. This implies $\overline{m} = 0$ because M/M' is $\mathbb{Z}_p$-free. Hence M/M' is torsion free as a $\mathbb{Z}_p[\zeta_{p^n}]$-module; moreover, M/M' is finitely generated over $\mathbb{Z}_p[\zeta_{p^n}]$ since it is finitely generated over $\mathbb{Z}_p$. Therefore M/M' is free of finite rank over $\mathbb{Z}_p[\zeta_{p^n}]$ since $\mathbb{Z}_p[\zeta_{p^n}]$ is a PID. □

Lemma 7. *Let $G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ for some prime p and some nonnegative integer n. Suppose M is a $\mathbb{Z}_pG$-module which is free of finite rank over $\mathbb{Z}_p$. Then there is a sequence $r_0, \dots, r_n$ of nonnegative integers such that for every subgroup $N_i = \langle g^{p^i} \rangle$ with $0 \leq i \leq n$ we have*

$$\operatorname{rank}_{\mathbb{Z}_p}(M^{N_i}) = \sum_{t=0}^{i} r_t \varphi(p^t)$$

and

$$\chi(N_i, M) = (n - i)\sum_{t=0}^{i} r_t \varphi(p^t) - p^i \sum_{t=i+1}^{n} r_t.$$

[1]Recall that if M is an R-module (R a commutative ring with 1), we say a submodule $N \leq M$ is R-pure when $rM \cap N \subseteq rN$ for every $r \in R$.

Proof. We use induction on n and Lemma 6. If $n = 0$, then $\mathbb{Z}_pG \cong \mathbb{Z}_p = \mathbb{Z}_p[\zeta_{p^0}]$ and $M \cong \mathbb{Z}_p[\zeta_{p^0}]^{r_0}$ is a free $\mathbb{Z}_p$-module for some nonnegative integer r_0, so the proposition is clear in this case since $0 \le i \le n = 0$ implies

$$\mathrm{rank}_{\mathbb{Z}_p}(M^{N_0}) = \mathrm{rank}_{\mathbb{Z}_p}(M) = r_0 = \sum_{t=0}^{0} r_t\varphi(p^t)$$

and

$$\chi(N_0, M) = 0 = (0-0)\sum_{t=0}^{0} r_t\varphi(p^t) - p^0 \sum_{t=1}^{0} r_t,$$

where

$$\sum_{t=1}^{0} r_t = 0$$

is an empty sum. Now suppose $n \ge 1$ and the proposition is true for $n-1$. By Lemma 6, we have a short exact sequence of $\mathbb{Z}_pG$-modules

$$0 \to M' \to M \to \mathbb{Z}_p[\zeta_{p^n}]^{\oplus r_n} \to 0$$

where M' can be regarded as a $\mathbb{Z}_pG'$-module where $G' = G/N_{n-1} \cong \mathbb{Z}/(p^{n-1})$. By induction, there is a sequence $r_0, \dots, r_{n-1}$ of nonnegative integers such that for every subgroup $N_i' = N_i/N_{n-1}$ with $0 \le i \le n-1$ we have

$$\mathrm{rank}_{\mathbb{Z}_p}(M^{N_i}) = \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i}) = \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i'}) = \sum_{t=0}^{i} r_t\varphi(p^t)$$

and

$$\chi(N_i', M') = (n-1-i)\sum_{t=0}^{i} r_t\varphi(p^t) - p^i \sum_{t=i+1}^{n-1} r_t$$

since $\mathbb{Z}_p[\zeta_{p^n}]^{N_i} = 0$. We need to compute the difference $\chi(N_i, M') - \chi(N_i', M')$, which we do using the inflation-restriction sequence. We get an exact sequence

$$0 \to H^1(N_i', M') \to H^1(N_i, M') \to H^1(N_{n-1}, M')^{N_i'} \to H^2(N_i', M') \to H^2(N_i, M')$$

where the last map in the sequence is multiplication by $1 + g^{p^{n-1}} + \dots + g^{p^{n-1}(p-1)}$; thus its cokernel is

$$\frac{M'^{N_i}}{(1 + g^{p^{n-1}} + \dots + g^{p^{n-1}(p-1)})M'^{N_i'}} = \frac{M'^{N_i}}{pM'^{N_i}}.$$

Therefore applying the p-adic order $\mathrm{ord}_p|-|$ to the exact sequence gives

$$\chi(N_i, M') - \chi(N_i', M') = \mathrm{ord}_p|M'^{N_i}/pM'^{N_i}| = \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i}) = \sum_{t=0}^{i} r_t\varphi(p^t)$$

since $H^1(N_{n-1}, M') = 0$. Hence

$$\begin{aligned}\chi(N_i, M) &= \chi(N_i, M') + r_n\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]) \\ &= \chi(N_i', M') + \sum_{t=0}^{i} r_t\varphi(p^t) + r_n\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]) \\ &= (n-i)\sum_{t=0}^{i} r_t\varphi(p^t) - p^i\sum_{t=i+1}^{n-1} r_t + r_n\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]),\end{aligned}$$

but $H^2(N_i, \mathbb{Z}_p[\zeta_{p^n}]) = 0$ and

$$H^1(N_i, \mathbb{Z}_p[\zeta_{p^n}]) = \frac{\mathbb{Z}_p[\zeta_{p^n}]}{(\zeta_{p^n}^{p^i} - 1)} \cong \frac{\mathbb{Z}_p[x]}{(x^{p^i} - 1) + (\Phi_{p^n}(x))} \cong \frac{\mathbb{Z}_p[\mathbb{Z}/(p^i)]}{(\Phi_{p^n}(1))} = \frac{\mathbb{Z}_p[\mathbb{Z}/(p^i)]}{(p)},$$

so $\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]) = -p^i$ as needed. Also, it is clear that $\chi(N_n, M) = 0$ and

$$\begin{aligned}\operatorname{rank}_{\mathbb{Z}_p}(M^{N_n}) &= \operatorname{rank}_{\mathbb{Z}_p}(M) \\ &= \operatorname{rank}_{\mathbb{Z}_p}(M') + r_n\operatorname{rank}_{\mathbb{Z}_p}(\mathbb{Z}[\zeta_{p^n}]) \\ &= \sum_{t=0}^{n-1} r_t\varphi(p^t) + r_n\varphi(p^n),\end{aligned}$$

which finishes the proof. □

Now we compute the $n+1$ unknown r_i's in Lemma 7 in terms of $n+2$ arithmetic invariants like lambda invariants and Euler characteristics of class groups.

Theorem 8. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. Suppose $\mu_{K_0} = 0$. Then $\mu_{K_1} = \cdots = \mu_{K_n} = 0$ and*

$$\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} = p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n})$$

where $G_n = \mathrm{Gal}(K_n/K_0)$.

Proof. Theorem 2 implies $\mu_{K_1} = \cdots = \mu_{K_n} = 0$ by induction. We apply Lemma 7 to the $\mathbb{Z}_pG_n$-module $A^*_{K_n}$ (the p-Pontryagin dual of the p-primary part of the class group), which is free of finite rank λ_{K_n} over $\mathbb{Z}_p$. Thus there is a sequence of nonnegative integers $r_0, r_1, \ldots, r_n$ such that for all $i = 0, 1, \ldots, n$ we have

$$\lambda_{K_i} = \operatorname{rank}_{\mathbb{Z}_p}(A^*_{K_i}) = \operatorname{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_i}) = \sum_{t=0}^{i} r_t\varphi(p^t)$$

$$\chi(G_n, A_{K_n}) = -\chi(N_0, A^*_{K_n}) = -nr_0 + \sum_{t=1}^{n} r_t$$

where $N_i = \mathrm{Gal}(K_n/K_i)$. Note that the natural map $C_{K_i} \to C_{K_n}^{N_i}$ has finite kernel and cokernel by the snake lemma, so indeed

$$\operatorname{rank}_{\mathbb{Z}_p}(A^*_{K_i}) = \operatorname{rank}_{\mathbb{Z}_p}((A_{K_n}^{N_i})^*) = \operatorname{rank}_{\mathbb{Z}_p}((A^*_{K_n})_{N_i}) = \operatorname{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_i}).$$

Hence

$$\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} = \sum_{i=0}^{n-1}\sum_{t=0}^{n-i} r_t\varphi(p^i)\varphi(p^t)$$

$$
\begin{aligned}
&= \sum_{i=0}^{n-1} \varphi(p^i) r_0 + \sum_{t=1}^{n} \sum_{i=0}^{n-t} \varphi(p^i)\varphi(p^t) r_t \\
&= \left(1 + (p-1)\sum_{j=0}^{n-2} p^j\right) r_0 + \sum_{t=1}^{n} r_t \varphi(p^t) \left(1 + (p-1)\sum_{j=0}^{n-t-1} p^j\right) \\
&= p^{n-1} r_0 + \varphi(p^n)(r_1 + \cdots + r_n) \\
&= p^{n-1}(1 + n(p-1)) r_0 + \varphi(p^n)(-n r_0 + r_1 + \cdots r_n) \\
&= p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n})
\end{aligned}
$$

which finishes the proof. □

Corollary 9. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. Suppose $\mu_{K_0} = 0$. Then*

$$
\lambda_{K_n} = p^n \lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i})
$$

where $G_i = \mathrm{Gal}(K_i/K_0)$.

Proof. We will use induction on n. First, it is clear that the statement holds when $n = 0$. Now take $n \geq 1$. Suppose the statement holds for all cyclic p-extensions of degree $\leq p^{n-1}$. Then by Theorem 8 we get

$$
\begin{aligned}
\lambda_{K_n} &= p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - \sum_{i=1}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} \\
&\overset{\text{induc.}}{=} p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) \\
&- \sum_{i=1}^{n-1} \varphi(p^i) \left(p^{n-i}\lambda_{K_0} + \varphi(p^{n-i})\chi(G_{n-i}, A_{K_{n-i}}) - (p-1)\sum_{j=1}^{n-i-1} \varphi(p^j)\chi(G_j, A_{K_j})\right) \\
&= p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - p^{n-1}(p-1)(n-1)\lambda_{K_0} \\
&- (p-1)\sum_{i=1}^{n-1} \varphi(p^{n-1})\chi(G_{n-i}, A_{K_{n-i}}) + (p-1)\sum_{i=1}^{n-1}\sum_{j=1}^{n-i-1} \varphi(p^i)\varphi(p^j)\chi(G_j, A_{K_j}) \\
&= p^n \lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\varphi(p^{n-1})\chi(G_{n-1}, A_{K_{n-1}}) \\
&- (p-1)\sum_{j=1}^{n-2} \varphi(p^{n-1})\chi(G_j, A_{K_j}) + (p-1)\sum_{j=1}^{n-2} \varphi(p^j)\left(\sum_{i=1}^{n-j-1} \varphi(p^i)\right)\chi(G_j, A_{K_j}) \\
&= p^n \lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\varphi(p^{n-1})\chi(G_{n-1}, A_{K_{n-1}}) \\
&- (p-1)\sum_{j=1}^{n-2} \varphi(p^j)p^{n-j-1}\chi(G_j, A_{K_j}) + (p-1)\sum_{j=1}^{n-2} \varphi(p^j)(p^{n-j-1} - 1)\chi(G_j, A_{K_j}) \\
&= p^n \lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\varphi(p^{n-1})\chi(G_{n-1}, A_{K_{n-1}}) \\
&- (p-1)\sum_{j=1}^{n-2} \varphi(p^j)\chi(G_j, A_{K_j})
\end{aligned}
$$

$$= p^n \lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\sum_{j=1}^{n-1} \varphi(p^j)\chi(G_j, A_{K_j})$$

as needed. □

Corollary 10. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. Suppose $\mu_{K_0} = 0$. Then*

$$p^{n-1}\chi(G_n, A_{K_n}) = \sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) + \sum_{i=1}^{n} p^{n-i}\chi(N_{i-1}/N_i, A_{K_i}).$$

where $N_i = \mathrm{Gal}(K_n/K_i)$ and again $G_i = \mathrm{Gal}(K_i/K_0)$.

Proof. We have

$$\begin{aligned} p^{n-1}\chi(G_n, A_{K_n}) &= \sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) + \frac{\lambda_{K_n} - p^n\lambda_{K_0}}{p-1} \\ &= \sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) + \sum_{i=1}^{n} p^{n-i}\chi(N_{i-1}/N_i, A_{K_i}) \end{aligned}$$

where the first equality follows from Corollary 9 and the second equality follows from induction on Iwasawa's formula 2.1. □

Corollary 11. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. As above, write $G_i = \mathrm{Gal}(K_i/K_0)$, $N_i = \mathrm{Gal}(K_n/K_i)$. Suppose $\mu_{K_0} = 0$. Then*

(1) for every $i = 0, \ldots, n$

$$\lambda_{K_n} \equiv \lambda_{K_i} \pmod{\varphi(p^{i+1})}$$

(2) we have

(a) in general,

$$\lambda_{K_n} \equiv -p^{n-1}\chi(G_n, A_{K_n}) - (p-1)\sum_{i=1}^{n-1}\varphi(p^i)\chi(G_i, A_{K_i}) \pmod{p^n},$$

(b) if $p \nmid n-1$,

$$\lambda_{K_n} \equiv \sum_{i=1}^{n-1} \frac{p^i(p-1)^2}{((i+1)p-i)(ip-i+1)}\chi(N_{n-i}, A_{K_n}) \pmod{p^n}$$

(3) also,

$$\mathrm{ord}_p|H^2(G_n, P_{K_n})| \le n\lambda_{K_0} + \mathrm{ord}_p|H^1(G_n, P_{K_n})| + \chi(G_n, I_{K_n})$$

Proof. For part (1), we only need to prove that for all $i = 1, \ldots, n$

$$\lambda_{K_i} \equiv \lambda_{K_{i-1}} \pmod{\varphi(p^i)}, \tag{11.1}$$

which we will do by induction on n. The base case $n = 1$ is clear from our restatement of Iwasawa's formula 5.1. Suppose then that Equation 11.1 holds for all $i < n$. Then for all $i = 1, \ldots, n-1$

$$p^{n-i}(\lambda_{K_i} - \lambda_{K_{i-1}}) \equiv 0 \pmod{\varphi(p^n)},$$

so

$$\begin{aligned}\lambda_{K_n} - \lambda_{K_{n-1}} &\equiv \lambda_{K_n} - \lambda_{K_{n-1}} + \sum_{i=1}^{n-1} p^{n-i}(\lambda_{K_i} - \lambda_{K_{i-1}}) \\ &= \sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} - p^{n-1}\lambda_{K_0} \\ &= p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - p^{n-1}\lambda_{K_0} \\ &= \varphi(p^n)\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) \equiv 0 \pmod{\varphi(p^n)}.\end{aligned}$$

For part (2), the first statement (a) follows immediately from Theorem 8 while the second statement (b) follows immediately from Theorem 13 below. To prove part (3), we note that

$$\begin{aligned}0 &\le \sum_{i=0}^{n-1} \frac{\lambda_{K_{n-i}} - \lambda_{K_{n-i-1}}}{\varphi(p^{n-i})} = \frac{1}{\varphi(p^n)} \sum_{i=0}^{n-1} p^i(\lambda_{K_{n-i}} - \lambda_{K_{n-i-1}}) \\ &= \frac{1}{\varphi(p^n)} \left(\sum_{i=0}^{n-1} p^i \lambda_{K_{n-i}} - \sum_{i=1}^{n} p^{i-1}\lambda_{K_{n-i}} \right) \\ &= \frac{1}{\varphi(p^n)} \left(\lambda_{K_n} + \sum_{i=1}^{n-1} (p^i - p^{i-1})\lambda_{K_{n-i}} - p^{n-1}\lambda_{K_0} \right) \\ &= \frac{1}{\varphi(p^n)} \left(\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} - p^{n-1}\lambda_{K_0} \right) \\ &= \frac{1}{\varphi(p^n)} \left(p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - p^{n-1}\lambda_{K_0} \right) \\ &= n\lambda_{K_0} - \chi(G_n, P_{K_n}) + \chi(G_n, I_{K_n}) \\ &= n\lambda_K - \mathrm{ord}_p|H^2(G, P_L)| + \mathrm{ord}_p|H^1(G, P_L)| + \chi(G, I_L),\end{aligned}$$

which finishes the proof. □

Remark 12. We can, of course, give a shorter, more direct proof of part (1) in Corollary 11 above. Namely, we apply Lemma 6 directly to get a short exact sequence

$$0 \to (A^*_{K_n})^{N_{n-1}} \hookrightarrow A^*_{K_n} \to \mathbb{Z}_p[\zeta_{p^n}]^{\oplus r} \to 0,$$

so

$$\lambda_{K_n} = \mathrm{rank}_{\mathbb{Z}_p}(A^*_{K_n}) = \mathrm{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_{n-1}}) + \mathrm{rank}_{\mathbb{Z}_p}(\mathbb{Z}_p[\zeta_{p^n}]^{\oplus r}) = \lambda_{K_{n-1}} + r\varphi(p^n)$$

as needed.

Now we relate the n Euler characteristics associated to subgroups (instead of quotients or subquotients)

$$\chi(N_0, A_{K_n}), \chi(N_1, A_{K_n}), \ldots, \text{ and } \chi(N_{n-1}, A_{K_n})$$

to the two lambda invariants λ_{K_n} and λ_{K_0}. The result is of a different nature since it involves non-integer coefficients.

Theorem 13. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. Suppose $\mu_{K_0} = 0$. Then $\mu_{K_1} = \cdots = \mu_{K_n} = 0$ and*

$$\frac{\lambda_{K_n} - p^n \lambda_{K_0}}{p-1} = \frac{p^n \chi(N_0, A_{K_n})}{np - n + 1} + \sum_{i=1}^{n-1} \frac{p^i (p-1) \chi(N_{n-i}, A_{K_n})}{((i+1)p - i)(ip - i + 1)}$$

where $N_i = \mathrm{Gal}(K_n/K_i)$.

The following lemma will make the proof of the above theorem much easier.

Lemma 14. *For all positive integers n we have*

$$\sum_{i=1}^{n-1} \frac{p^i (p-1) i}{((i+1)p - i)(ip - i + 1)} = \frac{p^{n-1} + p^{n-2} + \cdots + 1 - n}{np - n + 1}$$

and

$$\sum_{i=1}^{n-1} \frac{1}{((i+1)p - i)(ip - i + 1)} = \frac{n-1}{p(np - n + 1)}.$$

Proof. We use induction on n. If $n = 1$, then both right hand sides are zero and both left hand sides are empty sums, so the lemma is clear in this case. Now suppose that $n \geq 2$ and the statement is true for $n - 1$. Then

$$\begin{aligned}
&\sum_{i=1}^{n-1} \frac{p^i (p-1) i}{((i+1)p - i)(ip - i + 1)} \\
&= \frac{p^{n-1}(p-1)(n-1)}{(np - n + 1)((n-1)p - n + 2)} + \sum_{i=1}^{n-2} \frac{p^i (p-1) i}{((i+1)p - i)(ip - i + 1)} \\
&= \frac{p^{n-1}(p-1)(n-1)}{(np - n + 1)((n-1)p - n + 2)} + \frac{p^{n-2} + p^{n-3} + \cdots + 1 - (n-1)}{(n-1)p - n + 2} \\
&= \frac{p^{n-1}(p-1)(n-1) + \left(\frac{p^{n-1}-1}{p-1} - (n-1)\right)(np - n + 1)}{(np - n + 1)((n-1)p - n + 2)} \\
&= \frac{p^{n-1}(p-1)(n-1) + \left(\frac{p^{n-1}-1}{p-1} - (n-1)\right)(p-1)}{(np - n + 1)((n-1)p - n + 2)} + \frac{\frac{p^{n-1}-1}{p-1} - (n-1)}{np - n + 1} \\
&= \frac{(p^{n-1} - 1)(p-1)(n-1) + p^{n-1} - 1}{(np - n + 1)((n-1)p - n + 2)} + \frac{\frac{p^{n-1}-1}{p-1} - (n-1)}{np - n + 1} \\
&= \frac{p^{n-1} - 1}{np - n + 1} + \frac{p^{n-2} + p^{n-3} + \cdots + 1 - (n-1)}{np - n + 1} \\
&= \frac{p^{n-1} + p^{n-2} + \cdots + 1 - n}{np - n + 1}
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{i=1}^{n-1} \frac{1}{((i+1)p - i)(ip - i + 1)} \\
&= \frac{1}{(np - n + 1)((n-1)p - n + 2)} + \sum_{i=1}^{n-2} \frac{1}{((i+1)p - i)(ip - i + 1)}
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{(np-n+1)((n-1)p-n+2)} + \frac{n-2}{p((n-1)p-n+2)} \\
&= \frac{p+(n-2)(np-n+1)}{p(np-n+1)((n-1)p-n+2)} \\
&= \frac{p+(n-2)(p-1)+(n-2)((n-1)p-n+2)}{p(np-n+1)((n-1)p-n+2)} \\
&= \frac{(n-1)p-n+2+(n-2)((n-1)p-n+2)}{p(np-n+1)((n-1)p-n+2)} = \frac{n-1}{p(np-n+1)}
\end{aligned}$$

as claimed. □

Proof of Theorem 13. We may assume $n \geq 1$ since the statement is obvious in the case where $n = 0$ (both sides of the equation are zero). Lemma 7 implies that there are nonnegative integers $r_0, \ldots, r_n$ such that

$$\begin{aligned}
\lambda_{K_0} &= \operatorname{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_0}) = r_0, \\
\lambda_{K_n} &= \operatorname{rank}_{\mathbb{Z}_p}(A^*_{K_n}) = \sum_{t=0}^{n} r_t \varphi(p^t)
\end{aligned}$$

and

$$\chi(N_i, A_{K_n}) = -\chi(N_i, A^*_{K_n}) = -(n-i)\sum_{t=0}^{i} r_t\varphi(p^t) + p^i \sum_{t=i+1}^{n} r_t$$

for all $i \in \{0, \ldots, n\}$. On the one hand,

$$\frac{\lambda_{K_n} - p^n\lambda_{K_0}}{p-1} = \frac{\sum_{t=0}^{n} r_t\varphi(p^t) - p^n r_0}{p-1} = -(p^{n-1}+p^{n-2}+\cdots+1)r_0 + \sum_{t=1} r_t p^{t-1}.$$

On the other hand, the coefficient of r_0 occurring on the right hand side of the statement is

$$\begin{aligned}
&\frac{p^n}{np-n+1}(-n) + \sum_{i=1}^{n-1} \frac{p^i(p-1)(-i)}{((i+1)p-i)(ip-i+1)} \\
&= \frac{-np^n}{np-n+1} - \frac{p^{n-1}+p^{n-2}+\cdots+1-n}{np-n+1} \\
&= \frac{-np^n + n - \frac{p^n-1}{p-1}}{np-n+1} \\
&= \frac{-n(p-1)\frac{p^n-1}{p-1} - \frac{p^n-1}{p-1}}{np-n+1} \\
&= -\frac{p^n-1}{p-1} \\
&= -(p^{n-1}+p^{n-2}+\cdots+1)
\end{aligned}$$

and the coefficient of r_t for $t \geq 1$ is

$$\frac{p^n}{np-n+1} + \varphi(p^t)\sum_{i=1}^{n-t} \frac{p^i(p-1)(i)}{((i+1)p-i)(ip-i+1)} +$$

$$
\begin{aligned}
&p^n(p-1)\sum_{i=n-t+1}^{n-1}\frac{1}{((i+1)p-i)(ip-i+1)}\\
&=\frac{p^n}{np-n+1}-p^{t-1}(p-1)\frac{\frac{p^{n-t+1}-1}{p-1}-(n-t+1)}{(n-t+1)p-(n-t+1)+1}+\\
&p^n(p-1)\left(\frac{n-1}{p(np-n+1)}-\frac{n-t}{p((n-t+1)p-(n-t+1)+1)}\right)\\
&=\frac{p^n+p^{n-1}(p-1)(n-1)}{np-n+1}-\\
&\frac{p^t(p^{n-t+1}-1-(p-1)(n-t+1))+p^n(p-1)(n-t)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}-\frac{p^{n+1}-p^t((n-t+1)p-n+t)+(n-t)p^n(p-1)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}+p^{t-1}-\frac{p^{n+1}+(n-t)p^n(p-1)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}+p^{t-1}-p^n\frac{p+(n-t)(p-1)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}+p^{t-1}-p^{n-1}=p^{t-1},
\end{aligned}
$$

which completes the proof. □

4. An Alternative Proof of Lemma 7

Using a suggestion of Ralph Greenberg, we can use the structure theorem for finitely generated Λ-modules to give a different proof of Lemma 7.

Theorem 15. *Let M be a finitely generated Λ-module. Then there is a Λ-module homomorphism*

$$\theta\colon M\to\Lambda^r\oplus\bigoplus_{i=1}^{s}\frac{\Lambda}{(f_i(T)^{m_i})}\oplus\bigoplus_{j=1}^{t}\frac{\Lambda}{(p^{n_j})}$$

such that $\ker(\theta),\operatorname{coker}(\theta)$ *are finite and where each $f_i(T)\in\mathbb{Z}_p[T]$ is irreducible with $f_i(T)\equiv$ power of $T \pmod p$.*

We will see that Lemma 7 follows as an easy corollary of the following lemma.

Lemma 16. *Let $G=\langle g\rangle\cong\mathbb{Z}/(p^n)$ for some prime p and some nonnegative integer n. Suppose M is a $\mathbb{Z}_pG$-module which is free of finite rank over $\mathbb{Z}_p$. There is an injective $\mathbb{Z}_pG$-module homomorphism with finite cokernel*

$$M\rightarrowtail\bigoplus_{i=0}^{n}\mathbb{Z}_p[\zeta_{p^i}]^{\oplus r_i}$$

for some nonnegative integers $r_0,\ldots,r_n$ where each $\mathbb{Z}_p[\zeta_{p^i}]$ has $\mathbb{Z}_pG$-module structure given by

$$\mathbb{Z}_p[\zeta_{p^i}]\cong\frac{\mathbb{Z}_pG}{\Phi_{p^i}(g)\mathbb{Z}_pG}.$$

Proof. We know

$$\Lambda \cong \varprojlim_{m\in\mathbb{N}} \mathbb{Z}_p[\mathbb{Z}/(p^m)] \colon T \mapsto (g_m - 1)_{m\in\mathbb{N}}$$

with $\mathbb{Z}/(p^m) = \langle g_m \rangle$ written multiplicatively, so $\mathbb{Z}_pG$ is a quotient ring of Λ. In this way, every $\mathbb{Z}_pG$-module is a Λ-module with T acting as $g-1$, so Theorem 15 implies there is a Λ-module homomorphism

$$\theta \colon M \to \mathbb{Z}_p[[T]]^r \oplus \bigoplus_{i=1}^{s} \frac{\mathbb{Z}_p[[T]]}{(f_i(T)^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[[T]]}{(p^{n_j})}$$

such that $\ker(\theta), \operatorname{coker}(\theta)$ are finite and where each $f_i(T) \in \mathbb{Z}_p[T]$ is irreducible with $f_i(T) \equiv$ power of $T \pmod p$. Immediately, we see that $\ker(\theta) = 0$ since M is a free over $\mathbb{Z}_p$. If we tensor with $\mathbb{Q}_p$, we get an isomorphism

$$M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p[[T]]^{\oplus r} \oplus \bigoplus_{i=1}^{s} \frac{\mathbb{Q}_p[T]}{(f_i(T)^{m_i})}$$

of $\mathbb{Q}_p[T]$-modules, but $\dim_{\mathbb{Q}_p}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \operatorname{rank}_{\mathbb{Z}_p}(M) < \infty$ while $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p[[T]]) = \infty$, so $r = 0$. Now $x^{p^n} - 1$ kills the left hand side where $x := T + 1$, so $x^{p^n} - 1$ kills each

$$\frac{\mathbb{Q}_p[x]}{(h_i(x)_i^m)}$$

where $h_i(x) = f_i(x-1)$ is monic and irreducible. Hence each $h_i(x)^{m_i}$ divides $x^{p^n} - 1$ in $\mathbb{Q}_p[x]$, but $x^{p^n} - 1$ is the squarefree product of the (monic, irreducible) p^j-cyclotomic polynomials $\Phi_{p^j}(x)$ for $0 \le j \le n$, so every m_i is 1 and every $h_i(x)$ is $\Phi_{p^j}(x)$ for some $0 \le j \le n$. Hence our isomorphism becomes

$$M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{i=1}^{s} \frac{\mathbb{Q}_p[x]}{(h_i(x))} = \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Q}_p[x]}{(\Phi_{p^j}(x))} \right)^{\oplus r_j} \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Q}_pG}{\Phi_{p^j}(g)\mathbb{Q}_pG} \right)^{\oplus r_j}$$

as $\mathbb{Q}_pG$-modules for some nonnegative integers $r_0, \dots, r_n$. We have

$$\theta \colon M \rightarrowtail \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_p[[x]]}{(\Phi_{p^j}(x))} \right)^{\oplus r_j} \oplus \bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[[x]]}{(p^{n_j})},$$

but we know $\operatorname{im}(\theta)$ has trivial intersection with each $\mathbb{Z}_p[[x]]/(p^{n_j})$ factor since $p^{n_j} \nmid x^{p^n} - 1$, so there can be no such factors since $\operatorname{coker}(\theta)$ is finite while $\mathbb{Z}_p[[x]]/(p^m)$ is infinite when m is a positive integer. Also, since each $f_i(T) \equiv$ power of $T \pmod p$, we may apply a division algorithm (see Proposition 7.2 in [Was96]) to conclude

$$\frac{\mathbb{Z}_p[[x]]}{(h_i(x))} = \frac{\mathbb{Z}_p[[T]]}{(f_i(T))} \cong \frac{\mathbb{Z}_p[T]}{(f_i(T))} = \frac{\mathbb{Z}_p[x]}{(h_i(x))}$$

as $\mathbb{Z}_p[x]$-modules where again $x = T + 1$. Therefore

$$\theta \colon M \rightarrowtail \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_p[x]}{(\Phi_{p^j}(x))} \right)^{\oplus r_j} \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_pG}{\Phi_{p^j}(g)\mathbb{Z}_pG} \right)^{\oplus r_j}$$

is a $\mathbb{Z}_pG$-module homomorphism with finite cokernel. $\square$

Remark 17. Let $M, G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ be as in Lemma 16. We can now give another proof of Lemma 7. Observe that if C is a finite $\mathbb{Z}_pG$-module, then $\chi(N_i, C) = 0$ and $\mathrm{rank}_{\mathbb{Z}_p}(C^{N_i}) = 0$ for all $i \in \{0, \ldots, n\}$ where (as in 7) $N_i = \langle g^{p^i} \rangle$. Thus since χ and $\mathrm{rank}_{\mathbb{Z}_p}$ are additive on short exact sequences, we see that it suffices to note the following computations:

$$\mathbb{Z}_p[\zeta_{p^j}]^{N_i} = \begin{cases} \mathbb{Z}_p[\zeta_{p^j}] & \text{if } j \leq i \\ 0 & \text{if } j > i \end{cases}$$

$$\begin{aligned} \chi(N_i, \mathbb{Z}_p[\zeta_{p^j}]) &= \mathrm{ord}_p \left(\frac{|H^2(N_i, \mathbb{Z}_p[\zeta_{p^j}])|}{|H^1(N_i, \mathbb{Z}_p[\zeta_{p^j}])|} \right) \\ &= \begin{cases} \mathrm{ord}_p \left| \frac{\mathbb{Z}_p[\zeta_{p^j}]}{p^{n-i}\mathbb{Z}_p[\zeta_{p^j}]} \right| = (n-i)\varphi(p^j) & \text{if } j \leq i \\ \mathrm{ord}_p \left| \frac{\mathbb{Z}_p[\zeta_{p^j}]}{(1-\zeta_{p^j}^{p^i})\mathbb{Z}_p[\zeta_{p^j}]} \right|^{-1} = -p^i & \text{if } j > i. \end{cases} \end{aligned}$$

Remark 18. The proof of Lemma 16 and Theorem 8 show more than just formulas for Euler characteristics and lambda invariants. Indeed, they show a statement about representations. The proof is straightforward, so we shall forego it here.

Theorem 19. *Let $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields with $G_i = \mathrm{Gal}(K_i/K)$ and $N_i = \mathrm{Gal}(K_n/K_i) = \langle g^{p^i} \rangle \cong \mathbb{Z}/(p^i)$ for all $i = 0, \ldots, n$. Assume $\mu_K = 0$ and define*

$$V_{K_n} := A^*_{K_n} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

and let π_{K_n/K_0} be the corresponding representation. Then we have an isomorphism of $\mathbb{Q}_p$-representations (with the appropriate interpretation for negative coefficients)

$$\pi_{K_n/K_0} \cong \lambda_K \pi_{G_n} \oplus \bigoplus_{i=1}^{n} \left(\chi(G_i, A_{K_i}) - \chi(G_{i-1}, A_{K_{i-1}}) \right) \pi_{\varphi(p^i)}$$

where π_{G_n} is the regular representation and π_d is the unique faithful, irreducible representation of degree $d \in \{\varphi(p), \varphi(p^2), \ldots, \varphi(p^n)\}$.

5. Vanishing Criteria for Iwasawa Lambda Invariants

In this section we give a couple of generalized vanishing criteria for Iwasawa lambda invariants. The criteria will apply to certain cyclic extensions of $\mathbb{Z}_p$-fields of degree p^n and will generalize the results found in [FKOT97] of Fukuda et al. We need a couple of lemmas.

Lemma 20. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$. Suppose $\mu_K = \lambda_K = 0$. Then*

$$\mathrm{ord}_p|H^1(G, \mathcal{O}_L^\times)| + \mathrm{ord}_p|(I_L^G P_L)/(I_K P_L)| = \chi(G, I_L)$$

Proof. There is a short exact sequence of $\mathbb{Z}_pG$-modules

$$(I_K P_L^G)/I_K \rightarrowtail I_L^G/I_K \twoheadrightarrow I_L^G/(I_K P_L^G).$$

Also, $I_K \cap P_L^G = P_K$ since $P_L^G/P_K \cong H^1(G, \mathcal{O}_L^\times)$ being a p-group implies

$$(I_K \cap P_L^G)/P_K \subseteq P_L^G/P_K \subseteq A_K \cong 0$$

by our $\mu_K = \lambda_K = 0$ assumption. Thus using the third isomorphism theorem twice gives

$$\frac{I_K P_L^G}{I_K} \cong \frac{P_L^G}{I_K \cap P_L^G} = \frac{P_L^G}{P_K} \cong H^1(G, \mathcal{O}_L^\times)$$

and

$$\frac{I_L^G}{I_K P_L^G} = \frac{I_L^G}{I_L^G \cap (I_K P_L)} \cong \frac{I_L^G P_L}{I_K P_L}.$$

This completes the proof since

$$\mathrm{ord}_p |I_L^G / I_K| = \chi(G, I_L)$$

by the proof of Lemma 4. □

Now we can state and prove the first vanishing criterion.

Theorem 21. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place with $G = \mathrm{Gal}(L/K)$. Suppose $\mu_K = 0$. Then $\lambda_L = 0$ if and only if the following three conditions hold:*

(i) $\lambda_K = 0$
(ii) $\mathrm{ord}_p |H^2(G, \mathcal{O}_L^\times)| = 0$
(iii) $\mathrm{ord}_p |(I_L^G P_L)/(I_K P_L)| = 0$

Proof. Condition (i) is obviously necessary for $\lambda_L = 0$, so we may assume that $\lambda_K = 0$. Consider the tower

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

of $\mathbb{Z}_p$-fields where $G_i = \mathrm{Gal}(K_i/K) \cong \mathbb{Z}/(p^i)$ for all $i = 0, \ldots, n$. Then Lemma 20 and Lemma 4 imply

$$\begin{aligned} \chi(G_i, A_{K_i}) &= \mathrm{ord}_p |H^2(G_i, \mathcal{O}_{K_i}^\times)| - \mathrm{ord}_p |H^1(G_i, \mathcal{O}_{K_i}^\times)| + \chi(G, I_{K_i}) \\ &= \mathrm{ord}_p |H^2(G_i, \mathcal{O}_{K_i}^\times)| + \mathrm{ord}_p |(I_{K_i}^{G_i} P_{K_i})/(I_K P_{K_i})| \geq 0, \end{aligned}$$

for all $i = 1, \ldots, n$. Thus Corollary 9 shows that $\lambda_L = 0$ if and only if $\chi(G_i, A_{K_i}) = 0$ for all $i = 1, \ldots, n$, and the above computation proves that $\chi(G_i, A_{K_i}) = 0$ if and only if

$$\mathrm{ord}_p |H^2(G_i, \mathcal{O}_{K_i}^\times)| = \mathrm{ord}_p |(I_{K_i}^{G_i} P_{K_i})/(I_K P_{K_i})| = 0. \tag{21.1}$$

To complete the proof, it suffices to show that if Equation 21.1 holds for $i = n$, then it holds for all $i = 1, \ldots, n$. To show this it is enough to note that for all $i = 1, \ldots, n$ we have a surjection

$$\frac{\mathcal{O}_K^\times}{N_{L/K}(\mathcal{O}_L^\times)} \twoheadrightarrow \frac{\mathcal{O}_K^\times}{N_{K_i/K}(\mathcal{O}_{K_i}^\times)}$$

and an injection

$$\frac{I_{K_i}^{G_i} P_{K_i}}{I_K P_{K_i}} \rightarrowtail \frac{I_L^G P_L}{I_K P_L}$$

the 2nd of which follows by noting $(I_{K_i}^{G_i} P_{K_i}) \cap (I_K P_L) \subseteq I_{K_i} \cap (I_K P_L) \subseteq I_K P_{K_i}$. □

To derive our next lemma and establish the second vanishing criterion, we state the following result. A proof can be found, for example, in [Gre10].

Theorem 22. *Let ℓ/k be a Galois extension of number fields with $G = \mathrm{Gal}(\ell/k)$. Then there is an exact sequence of abelian groups*

$$0 \to \ker(J_{\ell/k}) \to H^1(G, \mathcal{O}_\ell^\times) \to \bigoplus_v \frac{\mathbb{Z}}{(e(w/v))} \to C_\ell^{[G]}/J_{\ell/k}(C_k) \to 0$$

where $C_\ell^{[G]}$ is the subgroup of C_ℓ^G generated by classes of G-fixed ideals, the direct sum ranges over all finite places v of k having ramification index $e(w/v)$ with w a place of ℓ lying over v, and

$$J_{\ell/k} \colon C_k \to C_\ell$$

is the natural map sending the class $[I]$ of an ideal I to the class $[\mathcal{O}_\ell I]$. Further, if G is cyclic and ℓ/k is unramified at every infinite place, then

$$\mathrm{q}(\mathcal{O}_\ell^\times) = \frac{|H^2(G, \mathcal{O}_\ell^\times)|}{|H^1(G, \mathcal{O}_\ell^\times)|} = \frac{1}{[\ell : k]}.$$

Lemma 23. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that $p \nmid h(k)$ and k has only one prime lying above p. Then*

$$\mathrm{ord}_p |H^2(G, \mathcal{O}_L^\times)| = 0.$$

where $G = \mathrm{Gal}(L/K)$.

Proof. Here we generalize the method of proof found in [FKOT97], where the result is proved in the case that L is totally real and $[L : K] = p$. First, note that if $\mathfrak{p}$ is the unique prime ideal of k lying over p, then $\mathfrak{p}_n/\mathfrak{p}$ is totally ramified in k_n/k and $p \nmid h(k_n)$ for all nonnegative integers n. Thus using Theorem 22 on the extension k_n/k_m with $G_{n/m} = \mathrm{Gal}(k_n/k_m)$ we find that for all nonnegative integers m, n with $m \leq n$

$$\begin{aligned}
\left| \frac{\mathcal{O}_{k_m}^\times}{N_{k_n/k_m}(\mathcal{O}_{k_n}^\times)} \right| &= |H^2(G_{n/m}, \mathcal{O}_{k_n}^\times)| = p^{-(n-m)} |H^1(G_{n/m}, \mathcal{O}_{k_n}^\times)| \\
&= p^{-(n-m)} e(\mathfrak{p}_n/\mathfrak{p}_m) \frac{|\ker(J_{k_n/k_m})|}{|C_{k_n}^{[G_{n/m}]}/J_{k_n/k_m}(C_{k_m})|} \\
&= p^{-(n-m)} p^{n-m} \frac{|C_{k_m}|}{\left| C_{k_n}^{[G_{n/m}]} \right|} = 1
\end{aligned}$$

where the last equality follows because $H^2(G_{n/m}, \mathcal{O}_{k_n}^\times)$ is a p-group and $\mathrm{ord}_p |C_{k_m}| = \mathrm{ord}_p |C_{k_n}^{[G_{n/m}]}| = 0$. Thus $N_{k_n/k_m}(\mathcal{O}_{k_n}^\times) = \mathcal{O}_{k_m}^\times$ for all nonnegative integers m, n with $m \leq n$, so if $L = \ell_\infty$ for some number field ℓ with $\mathrm{Gal}(\ell/k) \cong \mathrm{Gal}(L/K) \cong \mathbb{Z}/(p^d)$, then the induced maps

$$\widetilde{N}_{k_n/k_m} \colon \frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)} \longrightarrow \frac{\mathcal{O}_{k_m}^\times}{N_{\ell_m/k_m}(\mathcal{O}_{\ell_m}^\times)}$$

are surjective for all nonnegative integers m, n with $m \leq n$. On the other hand, using Theorem 22 on the extension ℓ_n/k_n with $G_n = \mathrm{Gal}(\ell_n/k_n) \cong \mathrm{Gal}(L/K) \cong$

$\mathbb{Z}/(p^d)$ we find

$$\begin{aligned}\left|\frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)}\right| &= |H^2(G_n, \mathcal{O}_{\ell_n}^\times)| = p^{-d}|H^1(G_n, \mathcal{O}_{\ell_n}^\times)| \\ &= p^{-d}\left(\prod_{i=1}^{s_n} e(w_i/v_i)\right)\frac{|C_{k_n}|}{\left|C_{\ell_n}^{[G_n]}\right|} \\ &= p^{-d}\left(\prod_{i=1}^{s_n} e(w_i/v_i)\right)\left|C_{\ell_n}^{[G_n]}\right|_p \\ &\leq p^{-d}p^{ds_\infty} = p^{d(s_\infty - 1)}\end{aligned}$$

where s_n is the number of ramified primes of k_n in ℓ_n/k_n and $s_\infty < \infty$ is the number of ramified primes of K in L/K. Therefore the maps $\widetilde{N}_{k_n/k_m}$ are isomorphisms of finite abelian groups for sufficiently large m, n. Now consider the canonical maps

$$\widetilde{\rho}_{k_n/k_m} : \frac{\mathcal{O}_{k_m}^\times}{N_{\ell_m/k_m}(\mathcal{O}_{\ell_m}^\times)} \longrightarrow \frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)}$$

for $m \leq n$. These maps have the property that $\widetilde{N}_{k_n/k_m} \circ \widetilde{\rho}_{k_n/k_m}$ is the exponentiation by p^{n-m} map when the groups are written multiplicatively. Thus when $n - m \geq d(s_\infty - 1)$ the composition $\widetilde{N}_{k_n/k_m} \circ \widetilde{\rho}_{k_n/k_m}$ is the trivial map, but $\widetilde{N}_{k_n/k_m}$ is an isomorphism for sufficiently large m, so $\widetilde{\rho}_{k_n/k_m}$ is the trivial map when m is sufficiently large and $n \geq m + d(s_\infty - 1)$. Therefore

$$H^2(G, \mathcal{O}_L^\times) \cong \varinjlim_n H^2(G_n, \mathcal{O}_{\ell_n}^\times) \cong 0$$

which finishes the proof. □

Now we are ready to give the more specialized and easily applicable vanishing criterion.

Theorem 24. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that p does not divide the class number of k and k has only one prime lying above p. Then $\lambda_L = 0$ if and only if, for all prime ideals $\mathfrak{p}$ of K which ramify in L/K and do not lie over p, the order in C_L of the class of the product of prime ideals of L lying over $\mathfrak{p}$ is prime to p.*

Proof. The "⇒" implication is clear. The "⇐" theorem follows from Theorem 21 by noting that (1) the assumptions we made ensure that conditions (i) and (ii) hold by Iwasawa's well-known vanishing criterion and Lemma 23, respectively, and (2) $(I_L^G P_L)/(I_K P_L)$ is a p-group generated by the classes of products of prime ideals of L lying over $\mathfrak{p}$ where $\mathfrak{p}$ runs through all prime ideals of K which ramify in L/K and do not lie above p. □

References

[AT09] E. Artin and J.T. Tate, *Class field theory*, AMS Chelsea Pub., 2009.

[FKOT97] Takashi Fukuda, Keiichi Komatsu, Manabu Ozaki, and Hisao Taya, *On Iwasawa λ_p-invariants of relative real cyclic extensions of degree p*, Tokyo J. Math. **20** (1997), no. 2, 475–480.

[Gre10] Ralph Greenberg, *Topics in Iwasawa theory*, math.washington.edu/, 2010.

[Iwa59] Kenkichi Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[Iwa73] ———, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[Iwa81] Kenkichi Iwasawa, *Riemann-Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. (2) **33** (1981), no. 2, 263–288.

[Was96] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Springer, 1996.